IC ON THE RECORD

Surveillance and Foreign Intelligence Gathering in the United States: The Current State of Play

Featuring comments from ODNI General Counsel Robert Litt and Director of the National Counterterrorism Center, Matthew Olsen.

November 19, 2013

On Tuesday November 19, 2013 Georgetown's Center on National Security and the Law and the National Security Law Society co-hosted the second event in a three part series: Surveillance and Foreign Intelligence Gathering in the United States: Past, Present and Future.

Introductory Remarks:

William Treanor - Dean, Georgetown Law

Keynote Address:

Representative Jim Sensenbrenner, R-Wisc.

Panelists:

Jameel Jaffer - Director, American Civil Liberties Union, Center for Democracy

Robert Litt - General Counsel, Office of the Director of National Intelligence

Matthew Olsen - Former General Counsel, National Security Agency

Marc Rotenberg - President and Executive Director, Electronic Privacy Information Center

Laura K. Donohue - Professor, Georgetown Law (moderator)

- #video
- #Robert Litt
- #Matthew Olsen
- #Jameel Jaffer
- #Marc Rotenberg
- #Laura K. Donohue
- #Georgetown Law
- #ACLU

- #ODNI
- #security
- #FISA
- #FISC
- #surveillance

- 3 months ago
- 2
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsq_y

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act

November 18, 2013

In June of this year, President Obama directed me to declassify and make public as much information as possible about certain sensitive programs while being mindful of the need to protect sensitive classified intelligence activities and national security. Since then, I have authorized the declassification and public release of numerous documents pertaining to the government's collection under Sections 501 and 702 of FISA.

Today I authorized the declassification and public release of additional documents relating to collection under Section 501, bringing the total to nearly 2000 pages of documents released to the public so far, including 20 orders and opinions of the Foreign Surveillance Court, 11 pleadings and other documents submitted to the Court, 24 documents provided to Congress, and 20 reports, training slides, and other internal documents describing the legal basis for the programs and how they operate. The information released today includes a number of internal NSA documents, training slides and internal guidance, which demonstrate the care with which NSA's foreign intelligence collection pursuant to Section 501 is run, managed, and overseen. Also included is the United States Signals Intelligence Directive 18 which details policies and procedures to ensure NSA's missions and functions are conducted in a manner that safeguards the constitutional rights of U.S persons, and two opinions from the Foreign Intelligence Surveillance Court concerning a now-discontinued NSA bulk electronic communications metadata program. These documents were properly classified and their declassification was not done lightly.

Release of these documents reflects the Executive Branch's continued commitment to making information about this intelligence collection program publicly available when appropriate and consistent with the national security of the United States. Additionally, they demonstrate the extent to which the Intelligence Community kept both Congress and the Foreign Intelligence Surveillance Court apprised of the status of the collection program under Section 215. Some information has been redacted because these documents include discussion of matters that continue to be properly classified for national security reasons and the harm to national security would be great if disclosed. These documents will be made available at the website of the Office of the Director of National Intelligence and at ICOntheRecord.tumblr.com, the public website dedicated to fostering greater public visibility into the intelligence activities of the U.S. Government.

James R. Clapper
Director of National Intelligence

Today's Releases

Training. The documents released today include a number of internal NSA documents, including training slides and internal guidance. These documents explain in detail rules that have been put in place to ensure compliance with the law and to protect privacy rights in conducting the NSA's signals intelligence mission. Together, these documents demonstrate the care with which NSA's foreign intelligence collection pursuant to Section 501 is run, managed, and overseen. Each of the training documents details the efforts that NSA makes to ensure that the restrictions under which NSA operates are ingrained in the workforce charged with implementing the authority granted by Congress and authorized by the FISC.

Minimization Procedures. In addition, as part of the Government's continuing effort to provide the public with additional information about how NSA conducts its activities, the DNI is publicly releasing United States Signal Intelligence Directive 18. This directive details policies and procedures designed to ensure that NSA's missions and functions are conducted as authorized by law and in a manner that is consistent with the Fourth Amendment to the Constitution. The directive sets forth the minimization policies and procedures regarding NSA's SIGINT activities, including the rules for the collection, retention, and dissemination of information about U.S. persons.

Electronic Communications Metadata Collection Opinions. Finally, the DNI has authorized the declassification and public release of two opinions of the FISC concerning a now-discontinued NSA bulk electronic communications metadata program. The FISC authorized this program under Section 402 of FISA, the Pen Register and Trap and Trace (PR/TT) provision. Previous public releases by the DNI, including the FISC's opinion from October 3, 2011, referenced this program, and the fuller explanation of the program provided by today's release extends the DNI's commitment to providing greater transparency for FISA activities. Except for a brief period, the FISC reauthorized this program approximately every 90 days from its inception until it was discontinued in 2011. Throughout its operation, the program was briefed to the Intelligence and Judiciary Committees of Congress and generally referenced in the then-classified white papers provided to Congress during reauthorization of the USA PATRIOT Act in 2009 and 2010.

The discontinued PR/TT program shared certain similarities to the NSA's bulk telephony metadata program—the subject of previous releases—in that the PR/TT program sought only the metadata associated with electronic communications and not their content; moreover, querying the metadata for both programs was permitted only for authorized counterterrorism purposes. Additionally, both programs operated with similar access, retention, and dissemination restrictions proposed by the Government and approved by the FISC. Given these operational similarities, many of the documents released today address both programs, sometimes side by side, even though, as noted above, the PR/TT program was conducted pursuant to a different legal authority from that authorizing the NSA's bulk telephony metadata program. At all times, the PR/TT program collected metadata from only a small percentage of world wide electronic communications traffic.

Additional Information on the Discontinued PR/TT Program

The Program

Under the now-discontinued PR/TT program, the FISC, after finding that the Government's applications satisfied the requirements of FISA and the Constitution, approved orders that enabled the Government to collect electronic communications metadata, such as the "to," "from," and "cc" lines of an email and the email's time and date. This program did not authorize the collection of the content of any electronic communications. Under this program, NSA could not read the content of any electronic communications for which the metadata was acquired. Like NSA's bulk telephony metadata program, this program was subject to several restrictions approved by the FISC, such as:

- The information had to be stored in secure databases.
- The information could be used only for counterterrorism purposes.
- The databases could be queried using an identifier such as an email address only when an analyst had a reasonable and articulable suspicion that the account or email address was associated with certain specified foreign terrorist organizations that were the subject of FBI counterterrorism investigations. The basis for that suspicion had to be documented in writing and approved by one of the 22 designated approving officials identified in the Court's Order. Moreover, if an identifier was reasonably believed to be used by a United States person, NSA's Office of General Counsel would also review the determination to ensure that suspected association was not based solely on First Amendment-protected activities.
- NSA was required to destroy the bulk metadata after a set period of time.

The Documents Released

The first PR/TT document released today is an opinion and order from the FISC that carefully analyzed and approved the Government's application to initiate this collection program. The Court's detailed 87-page opinion and 18-page order demonstrate the Court's searching and exhaustive review of the proposed program prior to its implementation. The opinion not only details the program's legal basis but also explains the procedures that NSA was required to follow in administering the program. The Court concluded that the NSA collection program was permissible under both FISA and the Constitution.

The second PR/TT document released today is a 117-page FISC opinion, which authorized NSA to re-initiate the program following the Government's suspension of the program for several months to address compliance issues identified by the Government and brought to the Court's attention. As the Court's opinion explains, these incidents involved three general categories of compliance issues: (1) access to the metadata; (2) disclosure of query results and information derived from them; and (3) overcollection. Because of the significance and complexity of these incidents, the Government did not seek an order from the FISC to renew the program when it expired on its normal schedule, thus essentially suspending the program for several months. As detailed in the opinion released today, the Government addressed these concerns during that period and, after a careful review, the FISC approved the Government's application to resume collection on a modified basis.

As previously stated, this electronic communications metadata bulk collection program has been discontinued. The Intelligence Community regularly assesses the continuing operational value of all of its collection programs. In 2011, the Director of NSA called for an examination of this program to assess its continuing value as a unique source of foreign intelligence information. This examination revealed that the program was no longer meeting the operational expectations that NSA had for it. Accordingly, after careful deliberation, the Government discontinued the program.

Both of these opinions contained extensive technical discussions of the particular means by which the collection was to be accomplished, particular targets of the collection, and other sensitive intelligence matters that must remain classified. Accordingly, they are being released in redacted form.

Executive Branch Initiatives

Upon discovery in 2009 of longstanding compliance issues associated with NSA's electronic communications and telephony bulk metadata collection programs, NSA recognized that its compliance and oversight structure had not kept pace with its operational momentum and the evolving and challenging technological environment in which it functioned. NSA, in close coordination with the Office of the Director of National Intelligence and the Department of Justice, therefore undertook significant steps to address these issues from a structural, managerial, and training perspective. The Director of NSA ordered comprehensive reviews of both of these collection programs to ensure that they were being implemented in accordance with all applicable legal requirements. Concurrently, NSA created the position of Director of Compliance to focus on the NSA-wide structural, managerial, and training improvements necessary to keep NSA's activities consistent with the law, policies, and procedures designed to protect privacy.

NSA continues to enhance training for both operational and technical personnel. NSA has added additional technology-based safeguards and has implemented procedures to ensure accuracy and precision in its filings before the FISC. NSA has also enhanced its oversight coordination with the Office of the Director of National Intelligence and the Department of Justice. NSA's senior leadership is directly involved in and responsible for compliance efforts across NSA, including regular senior leadership reviews of NSA's privacy compliance program.

Since 2009 and the discovery of the compliance incidents related to NSA's bulk metadata programs, the Government has continued to increase its focus on compliance and oversight. Today, NSA's compliance program is directly supported by over three hundred personnel, a threefold increase in just four years. This increase was designed to address changes in technology and authorities enacted as part of the FISA Amendments Act to confront evolving threats. This increase also reflects the commitment on the part of the Intelligence Community and the rest of the Government to ensuring that its intelligence collection activities are conducted responsibly and in accordance with the law.

The Government continues to evaluate whether additional information concerning the use of FISA authorities can be made public, consistent with protecting national security.

LIST OF RELEASES:

Reports to Congress

The Attorney General's Annual Reports on Requests for Access to Business Records under FISA for Years 2006-2012

- 2006
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012

April 10, 2009 NSA notification memorandum to SSCI on the status of the on-going NSA-initiated end-to-end review of its bulk telephony metadata programs conducted pursuant to Section 501 of FISA, and bulk electronic communications metadata program conducted pursuant to Section 402 of FISA.

June 29, 2009 NSA notification memorandum to HPSCI on the status of the on-going NSA-initiated end-to-end review of its bulk telephony metadata program conducted pursuant to Section 501 of FISA, and bulk electronic communications metadata program conducted pursuant to Section 402 of FISA.

December 1, 2010 NSA memorandum to SSCI explaining that NSA does not acquire cell site location information pursuant to the bulk electronic communications metadata program, and with the exception of a limited sampling for testing purposes, does not acquire such information pursuant to the bulk telephony metadata program.

Production to Congress of a May 23, 2006 Government Memorandum of Law in support of its Application to the FISC for authorization to conduct bulk telephony metadata collection under Section501 of FISA. Included with the Memorandum of Law is a copy of United States Signals Intelligence Directive 18 (USSID 18), which prescribes policies and procedures, and assigns responsibilities, to ensure that NSA's signals intelligence activities are conducted in a manner that is appropriate under the Fourth Amendment to the Constitution.

April 27, 2005 Prepared Testimony from Alberto R. Gonzales, Attorney General of the United States, and Robert S. Mueller, III, Federal Bureau of Investigation, United States Department of Justice Before the Select Committee on Intelligence discussing the government's use of USA PATRIOT Act authorities in combating international terrorism.

FISC Submissions, Opinions and Orders

Opinion of the FISC granting the Government's application seeking the collection of bulk electronic communications metadata pursuant to Section 402 of FISA, the Pen Register and Trap and Trace (PR/TT) provision.

Opinion of the FISC granting the Government's application seeking to re-instate NSA's bulk electronic communications metadata program following the Government's suspension of the program for several months to address compliance issues identified by the Government and brought to the Court's attention.

Order and Supplemental Order of the FISC (Updated 11/26/2013) in response to the Government's reporting of a compliance incident related to NSA's dissemination of certain query results discovered during NSA's end-to-end review of its bulk telephony metadata program, and ordering the Government to report on a weekly basis, any disseminations of information from that program outside of NSA and provide further explanation of the incident in its final report upon completion of the end-to-end review.

July 17, 2006 Court-ordered NSA Inspector General and General Counsel report on the adequacy of the management controls for the processing and dissemination of U.S. person information collected under NSA's bulk telephony metadata program. The report finds that although the NSA-designed management controls governing the processing, dissemination, security, and oversight of telephony metadata and U.S. person information are adequate, several aspects exceed the terms of the Court's Order, and proposes additional controls to enhance the protection of US person information.

August 17, 2006 NSA Presentation for the FISC regarding NSA's bulk telephony metadata program pursuant to Section 501 of FISA, and notification of two compliance issues concerning the collection.

September 1, 2009 NSA Presentation for the FISC regarding NSA's bulk telephony metadata program pursuant to Section 501 of FISA for the purpose of demonstrating NSA's compliance with the Court's Orders, and NSA's operational use of the bulk telephony metadata program in its counterterrorism missions while appropriately protecting privacy.

September 5, 2006 Cover filing submission to the FISC of the standard minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of information received by FBI pursuant to Section 501 of FISA.

May 8, 2009 Government Memorandum to the FISC providing preliminary notice of a compliance incident identified during the ongoing NSA-initiated end-to-end review of NSA's bulk telephony metadata program under Section 501 of FISA.

July 20, 2009 Order of the FISC approving the Government's request for authorization to provide the application and orders in docket number BR 06-05 to congressional committees consistent with the Government's congressional reporting requirements.

NSA Internal Procedures, Guidance, and Training Materials

United States Signals Intelligence Directive 18 Appendix J (USSID 18) dated April 24, 1986. (Relabeled previously posted document.)

United States Signals Intelligence Directive 18 (USSID 18) dated July 27, 1993, which prescribes policies and procedures designed to ensure that NSA's missions and functions are conducted as authorized by law in a manner that is consistent with the Fourth Amendment to the Constitution. The directive sets forth the minimization policies and procedures regarding NSA's SIGINT activities, including the rules for the collection, retention, and dissemination of information about U.S. persons. (**NOTE:** Document begins on page 29 of linked file).

United States Signals Intelligence Directive 18 (USSID 18) dated January 25, 2011, which prescribes policies and procedures designed to ensure that NSA's missions and functions are conducted as authorized by law in a manner that is consistent with the Fourth Amendment to the Constitution. The directive sets forth the minimization policies and procedures regarding NSA's SIGINT activities, including the rules for the collection, retention, and dissemination of information about U.S. persons.

Undated PowerPoint slide describing the requirements for verifying that only metadata, and not content, is collected consistent with Court order.

Undated NSA summary of requirements for the collection of bulk telephony metadata under Section 501 of FISA

January 8, 2007 NSA web—based training slides on NSA's bulk telephony metadata program pursuant to Section 501 of FISA. Topics include: 1) Court-ordered requirements; 2) the reasonable articulable suspicion (RAS) standard; 3) First Amendment considerations; and 4) Minimization procedures governing the accessing, sharing, retention, and dissemination of information.

January 8, 2007 Interim Competency Test for NSA analysts on legal and compliance issues concerning queries of bulk telephony metadata acquired by NSA pursuant to Section 501 of FISA.

January 8, 2007 NSA PowerPoint presentation, designed for use by NSA personnel with access to the bulk telephony metadata acquired by NSA pursuant to Section 501 of FISA, for purposes of performing analytical functions, including:

(1) Court-ordered requirements;
(2) The reasonable articulable suspicion (RAS) standard;
(3) First Amendment considerations; and
(4) Minimization procedures governing the accessing, sharing, retention, and dissemination of information.

August 2009 NSA Cryptological School Course on Legal, Compliance, and Minimization Procedures. These course materials, designed for NSA personnel provided access to bulk telephony and electronic communications metadata acquired pursuant to Section 501 of FISA and Section 402 of FISA respectively, include:

(1) Background on constitutional constraints under the Fourth Amendment for NSA collection activities;
(2) Legal framework and applicable standards for collection, retention, dissemination of information under FISA and Executive Order 12333;
(3) Guidance on collection, processing, retention, and dissemination of information under United States Signals Intelligence Directive 18 (USSID 18); and
(4) Oversight and compliance issues relating to access and use of SIGINT databases and information.

August 29, 2008 NSA memorandum providing guidance on NSA policy as to the applicable legal standards for querying bulk telephony metadata acquired pursuant to Section 501 of FISA, and bulk electronic communications metadata acquired pursuant to Section 402 of FISA.

September 2008 Attorney General's Guidelines for Domestic FBI Operations, which establishes the framework for the use of authorities and investigative methods to protect the United States from terrorism and other threats to the national security, and to further United States foreign intelligence objectives, in a manner consistent with the Constitution and laws of the United States.

NSA Core Intelligence Oversight Training materials relating to NSA signals intelligence collection activities, including:

(1) Executive Order 12333;
(2) December 1982 DOD Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons (DoD 5240 1-R);

(3) NSA/Central Security Service (CSS) Policy 1-23, Procedures Governing NSA/CSS Activities that Affect U.S. Persons, which establishes procedures and assigns responsibilities to ensure that the signals intelligence and information assurance missions of NSA and the Central Security Service are conducted in a manner consistent with the privacy rights of U.S. persons as required by law, executive orders, DOD policies and instructions, and internal policy; and
(4) DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters (DTM 08-052).

2011 NSA Course Materials regarding NSA's bulk telephony metadata program pursuant to Section 501 of FISA, and NSA's bulk electronic communications metadata program pursuant to Section 402 of FISA. These materials contrast the differences between the authorities granted for the two programs, detail the limitations on accuse, use, and retention of information collected under these two programs, and explain the role of the two programs in the context of the broader set of NSA's SIGINT authorities.

- Introduction
- Module 1
- Module 2
- Module 3
- Module 4
- Module 5
- Module 6 (for Analytic Personnel)
- Module 6 (for Technical Personnel)

- #declassified
- #NSA
- #metadata
- #Section 501
- #Section 215
- #FISA
- #FISC
- #ODNI
- #DNI Clapper
- #minimization

- 3 months ago
- 18
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsq_c

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

ODNI General Counsel Robert Litt's as prepared statement for the record before the Joint Hearing of the Privacy, Technology and the Law Subcommittee of the Senate Judiciary Committee

Subject: "The Surveillance Transparency Act of 2013"

Chaired by: Senator Al Franken (D-MN)

Witnesses:

Senator Dean Heller (R-NV)
Robert Litt, General Counsel in the Office of the Director of National Intelligence (ODNI)
Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Dept. of Justice

Location: 226 Dirksen Senate Office Building, Washington, D.C.

Date: Wednesday, November 13, 2013: Time: 10:03 a.m. EST

Thank you, Mr. Chairman, Ranking Member Flake, Senator Blumenthal. Thank you for the opportunity to appear before you today to discuss this very important issue of how best to inform the public about sensitive intelligence activities consistent with the need of national security.

And I want to say that I appreciate the support that you have shown for the intelligence community over the last few months and their activities.

The recent unauthorized disclosures have led to a public dialogue about intelligence collection activities, particularly those conducted under the Foreign Intelligence Surveillance Act. But it is critical to ensure that that public dialogue is grounded in fact rather than in misconceptions; and therefore, we agree that it's important to help the public understand how the intelligence community uses the legal authorities that Congress has provided it to gather foreign intelligence, and the vigorous oversight of those activities to ensure that they comply with the law.

As you know, some months ago, the president directed the intelligence community to make as much information as possible about certain intelligence programs that were the subject of those unauthorized disclosures available to the public, consistent with the need to protect national security and sensitive sources and methods.

Since then, the director of national intelligence has declassified and released thousands of pages of documents about these programs, and we're continuing to review documents to release more of them.

These documents demonstrate that these programs are all authorized by law and subject to vigorous oversight by all three branches of government.

And it's important to emphasize that this information was properly classified. It's being declassified now only because in the present circumstances the public interest in declassification outweighs the national security concerns that required classification. But we still have to take those national security concerns into account.

In addition to declassifying documents, we've also taken significant steps to allow the public to know the extent to which we use the authorities under FISA. And I agree with both of you and Senator Heller that it is appropriate to find ways to inform the public about this consistent with national security.

Specifically, as we set out in more detail in our written statement for the record, the government is going to release on an annual basis the total number of orders issued under

various FISA authorities and the total number of targets affected by those orders.

Moreover, recognizing that it's important for the companies to be able to reassure their customers about how often or, more precisely, how rarely the companies actually provide information about their customers to the government, we've agreed to allow them to report the total number of law enforcement and national security legal demands they receive each year and the number of accounts affected by those orders.

We believe that this approach strikes the proper balance between providing the public information about the use of the legal authorities and protecting our important collection capabilities. And I'd be glad to discuss that with you in more detail as we move ahead.

Turning to the Surveillance Transparency Act of 2013, which you and Senator Heller have cosponsored, we've reviewed the bill and we share the goal of providing the public greater insight into the government's use of FISA authorities. And we appreciate the effort that you've made in this bill to try to accommodate transparency and national security. We've had good discussions with your staff about that bill.

Many of the bill's provisions are consistent with the steps we've taken so far, and we support them. But we do continue to have concerns that some of the provisions raise significant operational or practical problems. These concerns are summarized or are set out in more detail in the written statement for the record. And I'll just summarize here and now that they fall into two broad categories.

First, while we believe it is possible and appropriate to reveal information about the number of targets of surveillance, counting the number of persons or of U.S. persons whose communications are actually collected, even if they're not the targets, is operationally very difficult, at least without an extraordinary investment of resources and maybe not even then.

For example, it's often not possible to determine whether a person who receives an email is a U.S. person. The email address says nothing about the citizenship or nationality of that person.

And even in cases where we would be able to get the information that would allow us to make the determination of whether someone is a U.S. person, doing the research and collecting that information would perversely require a greater invasion of that person's privacy than would otherwise occur.

It's for these reasons that the inspectors general of the National Security Agency and of the intelligence community have stated in letters to the Congress that this kind of information simply cannot be reasonably obtained.

Second, we have significant concerns with allowing individual companies to report information about the number of orders to produce the data that they receive under particular provisions of the law. Providing that information in that level of detail could provide our adversaries a detailed road map of which providers and which platforms to avoid in order to escape surveillance.

We believe that the reporting we've already agreed to provides the right balance between transparency and national security.

Mr. Chairman, I want to emphasize our intention to work with the Congress and with this committee to ensure the maximum possible transparency about our intelligence activities that's consistent with national security. The president is committed to this; the director of national intelligence is committed to this; the attorney general is committed to this; General Alexander is committed to this.

We're open to considering any proposals so long as they do not compromise our ability to collect the information we need to protect this nation and our allies. And we look forward to working with you in this regard.

Thank you.

- #statement
- #Robert Litt
- #Congressional Oversight
- #Senator Franken
- #Senate Judiciary Committee
- #FISA
- #NSA
- #Surveillance Transparency Act of 2013
- #ODNI

- 3 months ago
- 3
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsq_

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

NSA's Activities:

Valid Foreign Intelligence Targets Are the Focus

October 31, 2013

Recent press articles on NSA's collection operations conducted under Executive Order 12333 have misstated facts, mischaracterized NSA's activities, and drawn erroneous inferences about those operations. NSA conducts all of its activities in accordance with applicable laws, regulations, and policies – and assertions to the contrary do a grave disservice to the nation, its allies and partners, and the men and women who make up the National Security Agency.

All NSA intelligence activities start with a validated foreign intelligence requirement, initiated by one or more Executive Branch intelligence consumers, and are run through a process managed by the Office of the Director of National Intelligence. When those requirements are received by NSA, analysts look at the Information Need and determine the best way to satisfy it. That process involves identifying the foreign entities that have the information, researching how they communicate, and determining how best to access those communications in order to get the foreign intelligence information. The analysts identify selectors – e-mail addresses and phone numbers are examples – that help isolate the communications of the foreign entity and task those to collection systems. In those cases where there are not specific selectors available, the analysts will use metadata, similar to the address on the outside of an envelope, to attempt to develop selectors for their targets. Once they have them, they task the selectors to the collection systems in order to get access to the content, similar to the letter inside the envelope.

The collection systems target communications links that contain the selectors, or are to and from areas likely to contain the selectors, of foreign intelligence interest. Seventy years ago, the communications links were shortwave radio transmissions between two points on the globe. Today's communications flow over technologies like satellite links, microwave towers, and fiber optic cables. Terrorists, weapons proliferators, and other valid foreign intelligence targets make use of commercial infrastructure and services. When a validated foreign intelligence target uses one of those means to send or receive their communications, we work to find, collect, and report on the communication. Our focus is on targeting the communications of those targets, not on collecting and exploiting a class of communications or services that would sweep up communications that are not of bona fide foreign intelligence interest to us.

What NSA does is collect the communications of targets of foreign intelligence value, irrespective of the provider that carries them. U.S. service provider communications make use of the same information super highways as a variety of other commercial service providers. NSA must understand and take that into account in order to eliminate information that is not related to foreign intelligence.

NSA works with a number of partners and allies in meeting its foreign-intelligence mission goals, and in every case those operations comply with U.S. law and with the applicable laws under which those partners and allies operate. A key part of the protections that are provided to both U.S. persons and citizens of other countries is the requirement that information be in support of a valid foreign intelligence requirement, and the Attorney General-approved minimization procedures. These limitations protect the privacy of all people and, in particular, to any incidentally acquired communications of U.S. persons. The protections are applied when selectors are tasked to the collection system; when the collection itself occurs; when the collected data are being processed, evaluated, analyzed, and put into a database; and when any reporting of the foreign intelligence is being done. In addition, NSA is very motivated and actively works to remove as much extraneous data as early in the process as possible – to include data of innocent foreign citizens.

NSA Public Affairs Office

- #statement
- #NSA
- #selectors
- #EO 12333
- #metadata
- #telecommunications
- #ODNI
- #DOJ
- #collection systems

- 3 months ago
- 13
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqz

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

American Bar Association

23rd Annual Review of the Field of National Security Law

Executive Updates on Developments in National Security Law

Panel: Privacy, Technology and National Security: An Overview of Intelligence Collection

As Prepared Remarks of Robert S. Litt General Counsel for the Office of the Director of National Intelligence

October 31, 2013

Not surprisingly, the two major issues that have been occupying my time recently have been budget issues and the fallout from the Snowden leaks.

I spent the first part of October working almost entirely alone in our office, supported just by my deputy, advising on who was allowed to work and what they were allowed to do.

And also responding to inquiries from people who did not seem to comprehend that when (a) Congress prohibits personnel from working when they aren't paid, and (b) the Intelligence Community isn't appropriated funds to pay personnel, then (c) most IC personnel won't be able to work.

But even before the shutdown, the Intelligence Community was feeling the pinch of sequestration.

We recognize that in the current budgetary environment, the IC, along with the rest of the government, will have to endure some cuts. The problem with sequestration is that, rather than allowing us to make cuts in a sensible manner, based on mission needs, it requires us to cut everything across the board.

We were able to deal with sequestration in the past year by delaying or deferring some activities and reprogramming funds to cover critical gaps.

But this fiscal year, sequestration will require another round of cuts, and we won't have the same flexibility to deal with them.

Instead of short-term delays or creative mitigation strategies, we will be forced to cut capabilities

Instead of determining what capabilities we need to keep the country safe, we will be forced to determine what capabilities we can afford to provide.

The impact of sequestration will likely open new intelligence gaps and prevent us from mitigating existing ones.

So we are hopeful that the Congress will find a way to avoid sequestration for this year, though we recognize that that is by no means a certain outcome.

Obviously, however, since June the bulk of my time has been spent dealing with leaks about our surveillance activities.

I want to address a couple of big picture issues about this topic.

For one thing, I'd like to provide a sort of "user's guide" for people who follow this in the press.

Begin with the proposition that you shouldn't believe everything you read or hear, and I mean that literally.

The media reports are often based on documents that are exceptionally complicated, dense and jargonized, and require a level of technical knowledge that most people, including me, don't have. And the documents often present only part of the story.

On top of that, even when reporters come to us for comment – and they don't always – we frequently cannot correct their mistakes without compromising sensitive sources and methods.

A good example of what I am talking about is the story last week that claimed that we had collected 70 million French telephone calls in a month.

That was simply untrue, because the reporter didn't understand what he was looking at. As has now been made public, these 70 million calls were in fact collected by the French intelligence service, outside of France, in furtherance of mutual counterterrorism and force protection concerns, and provided by the French intelligence service to us.

But until the truth was leaked to the Wall Street Journal, we couldn't correct this publicly, to avoid damaging sensitive intelligence relationships. That's the kind of problem we face.

Second, a lot of these stories have focused on the raw technical capabilities of the U.S. intelligence community. And yes, those capabilities are considerable. But it is important to differentiate between technical capability and actual practice – between what might be done and what is actually done – between what we can do technically and what we can do legally.

For example, there have been stories claiming that NSA is able to crack encryption or break into private networks, and charges that this compromises everyone's privacy.

I'm not going to comment on whether or not these stories were accurate.

But isn't cracking encryption, or breaking into private networks, exactly what we want an intelligence agency to be able to do?

How else are we going to collect the communications of people who want to harm us and our allies, and who use those tools to try to hide their communications, or to provide policy makers the intelligence they need to protect the nation?

But just because we try to develop the capability to intercept and decrypt communications of adversaries and terrorists does not mean that we can or do use those capabilities against ordinary U.S. citizens, or French citizens, or Belgians, etc.

Our intelligence agencies are the best in the world, but – and this is the key point – they only conduct surveillance to the extent they are allowed to by the law, and that includes that they do not target the communications of Americans except as specifically authorized by the law, and cannot target foreigners except for a valid foreign intelligence purpose.

And this leads to another big picture point. Everything that has been exposed so far has been done within the law.

We get court orders when we are required to, we minimize information about U.S. persons as we are required to, we collect intelligence for valid foreign intelligence purposes as we are required to.

And, unlike many other countries which engage in the same types of collection activities, our intelligence services are subject to multi-layered oversight, which includes oversight by Executive agencies, Congress and judicial authorities. As you have seen in FISA Court documents, that oversight is not pro forma. Errors are reported. Independent fact finding is conducted. Hearings are held and remedies are imposed. Congress is briefed.

We also have extensive technical systems that help us ensure that the rules are complied with.

Even though we aren't always perfect – even though technical and human failures can lead to compliance problems – nothing has come out that indicates that there has been any intentional abuse of our surveillance capabilities.

This is a far cry from, say, the illegal domestic surveillance of the 1960s and 1970s.

I recognize that there are people who believe that the law should be different, and they have advocated that position forcefully.

But – for example – the bulk telephony metadata program has been conducted pursuant to over 30 court orders by over a dozen separate judges.

The last two renewals were after the public controversy erupted, and in the face of all of the arguments that have been made against the program.

If the law changes, we'll follow the new law; but for now, we'll follow the law as Congress passed it and the courts interpret it.

Finally, I want to talk about the implications of the last few months for how we authorize and oversee classified intelligence activities.

These disclosures have started a public debate about the appropriate scope of surveillance.

But this debate comes with a cost, and the cost is that to the extent we are exposing what our intelligence agencies can do, we make it harder for them to do it. What the Washington Post reports, al Qaeda knows.

For over thirty years, we've had a consensus about how to balance the need for secrecy in intelligence programs with the need for oversight of those programs.

We did this through the congressional intelligence committees, which were set up precisely for this purpose. We are required by law to keep them fully and currently informed about all intelligence activities, and we do.

The committees have stood as proxies for the American people, to avoid the harm to our national security that would come from full public disclosure of our activities, while ensuring that elected representatives of the people oversee those activities.

The last few months have provided a different model of oversight – one in which private individuals, without visibility into or responsibility for protecting the nation, are making their own judgments about what should and should not be disclosed, and one in which the general public is debating what our intelligence agencies should and should not do.

Some might argue that there are benefits from this approach. It provides more transparency for the public and allows public debate about matters that typically have been kept secret.

But I want to end with two important issues that we need to think about.

One is – is oversight by the committee of the whole really the optimal way to conduct intelligence oversight? Or will the costs to our national security outweigh the benefits of disclosure?

And the second is that the intelligence community must acknowledge how difficult it is to keep secrets today. In determining what activities to undertake we need to give more consideration to what the impact of additional leaks would be. In each case we have to assess, to a greater extent than we have to date – is the game worth the candle?

The President has directed a review of our intelligence programs, in part with this issue in mind, and I think that that review, and any follow on actions, are certainly going to be occupying my time in the next year.

- #speeches and interviews
- #robert litt
- #Edward Snowden

- #sequestration
- #encryption
- #surveillance

- 3 months ago
- 9
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqz8

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

Remarks as delivered by James R. Clapper Director of National Intelligence

Open Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act to the House Permanent Select Committee on Intelligence

October 29, 2013

HVC 210, Capitol, Washington, D.C.

Well, Mr. Chairman, I will go ahead with our prepared statements on FISA legislation, and then we can certainly get to questions that we know you all have.

So, Chairman Rogers, Ranking Member Ruppersberger, distinguished members of the Committee. Thanks so much for having us here today, to talk about the way ahead, occasioned by the continuing dramatic revelations about intelligence collection programs since their unauthorized disclosure [BREAK AS PROTESTOR IS REMOVED].

And about the steps we're taking to make these programs more transparent, while still protecting our national security interests. We each have statements, so I'll begin, and then transition to General Alexander.

This hearing is a key part of the discussion our nation needs, about legislation that provides the Intelligence Community with authorities, both to collect critical foreign intelligence, and to protect privacy and civil liberties.

We – all of us – in the Intelligence Community, are very much aware that the recent unauthorized disclosures have raised serious concerns that you alluded to, both here in Congress, and across the nation, about our intelligence activities.

We know the public wants to understand how its Intelligence Community uses its special tools and authorities, and to judge whether we can be trusted to use them appropriately. We believe we have been lawful, and that the rigorous oversight we've operated under has been effective. So we welcome this opportunity to make our case to the public.

As we engage in this discussion, I think it's also important that our citizens know that the unauthorized disclosure of the details of these programs has been extremely damaging. From my vantage, as DNI, these disclosures are threatening our ability to conduct intelligence, and to keep our country safe. There's no way to erase, or make up for, the damage that we know has already been done, and we anticipate even more, as we continue our assessment – and as more revelations are made.

Before these unauthorized disclosures, we were always very conservative about discussing the specifics of our collection programs, based on the truism that the more adversaries know about what we're doing, the more they can avoid our surveillance. But the disclosures, for better or for worse, have lowered the threshold for discussing these matters in public. So, to the degree that we can discuss them, we will.

But this public discussion should be based on an accurate understanding of the Intelligence Community: Who we are, what we do, and how we're overseen.

In the last few months, the manner in which our activities have been characterized has often been incomplete, inaccurate, or misleading, or some combination thereof.

I believe that most Americans realize the Intelligence Community exists to collect the vital intelligence that helps protect our nation from foreign threats. We focus on uncovering the secret plans and intentions of our foreign adversaries, as we've been charged to do.

But what we do not do is spy unlawfully on Americans, or for that matter, spy indiscriminately on the citizens of any country. We only "spy" for valid foreign intelligence purposes, as authorized by law, with multiple layers of oversight, to ensure we don't abuse our authorities.

Unfortunately, this reality has sometimes been obscured in the current debate. And for some, this has led to a erosion of trust in the Intelligence Community.

And we do understand the concerns on the part of the public. I'm a Vietnam veteran, and I remember, as Congressional investigations of the 1970s later disclosed – and I was in the Intelligence Community then – that some intelligence programs were carried out for domestic political purposes, without proper legal authorization or oversight.

But having lived through that, as a part of the Intelligence Community, I can now assure the American people that the Intelligence Community of today is not like that. We operate within a robust framework of strict rules and rigorous oversight, involving all three branches of the government.

Another useful historical perspective, I think, is that during the Cold War, the Free World and the Soviet bloc had mutually exclusive telecommunications systems, which made foreign collection a lot easier to distinguish.

Now, world telecommunications are unified. Intertwined with hundreds of millions of innocent people, conducting billions of innocent transactions, are a much smaller number of nefarious adversaries who are trying to do harm on the very same network, using the very same technologies. So, our challenge is to distinguish, very precisely, between these two groups of communicants.

If we had an alarm bell that went off whenever one terrorist communicated with another terrorist, our jobs would be infinitely easier. But that capability just doesn't exist in the world of technology, at least today.

Over the past months, I've declassified and publicly released a series of documents related to both Section 215 of the PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, or FISA.

We're doing that to facilitate informed public debate about the important intelligence collection programs that operate under these authorities. We felt that in light of the unauthorized disclosures, the public interest in these documents far outweighed the potential additional damage to national security.

These documents let our citizens see the seriousness, the thoroughness, and the rigor with which the FISA Court exercises its responsibilities. They also reflect the Intelligence Community's – particularly NSA's – commitment to uncovering, reporting, and correcting any compliance matters that occur. However, even in these documents, we've had to redact certain information to protect sensitive sources and methods, such as particular targets of surveillance.

But we will continue to declassify more documents. That's what the American people want, it's what the President has asked us to do, and I personally believe it's the only way we can reassure our citizens that their Intelligence Community is using its tools and authorities appropriately.

The rules and oversight that govern us ensure we do what the American people want us to do, which is protect our nation's security and our people's liberties.

So I'll repeat: We do not spy on anyone except for valid foreign intelligence purposes, and we only work within the law. Now to be sure, on occasion, we've made mistakes – some quite significant. But these are usually caused by human error or technical problems. And whenever we've found mistakes, we've reported, addressed, and corrected them.

The National Security Agency specifically, as part of the Intelligence Community broadly, is an honorable institution. The men and women who do this sensitive work are honorable people, dedicated to conducting their mission lawfully, and are appalled by any wrongdoing. They, too, are citizens of this nation, who care just as much about privacy and constitutional rights as the rest of us. They should be commended for their crucial and important work in protecting the people of this country, which has been made all the more difficult by the torrent of unauthorized, damaging disclosures.

That all said, we in the IC stand ready to work in partnership with you, to adjust foreign surveillance authorities, to further protect our privacy and civil liberties. And I think there are some principles we already agree on.

First, we must always protect our sources, methods, targets, partners, and liaison relationships.

[Second,] We must do a better job in helping the American people understand what we do, why we do it, and, most importantly, the rigorous oversight that helps ensure we do it correctly.

And third, we must take every opportunity to demonstrate our commitment to respecting the civil liberties and privacy of every American.

But, we also have to remain mindful of the potential negative long-term impact of over-correcting the authorizations granted to the Intelligence Community. As Americans, we face an unending array of threats to our way of life, more than I've seen in my 50 years in intelligence. And we need to sustain our ability to detect these threats.

We certainly welcome a balanced discussion about national security and civil liberties. It's not an either/or situation; we need to continue to protect both.

So with that, let me turn to General Alexander.

- #DNI Clapper
- #testimony
- #NSA
- #metadata
- #FISA
- #FISC
- #HPSCI
- #Congressional Oversight
- #Mike Rogers
- #Dutch Ruppersberger

- 3 months ago
- 4
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqz2

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act

October 28, 2013

In June of this year, President Obama directed me to declassify and make public as much information as possible about certain sensitive intelligence collection programs undertaken under the authority of the Foreign Intelligence Surveillance Act (FISA) while being mindful of the need to protect national security. Consistent with this directive, in September 2013, I authorized the declassification and public release of a number of documents pertaining to the Government's collection of bulk telephony metadata under Section 501 of the FISA, as amended by Section 215 of the USA PATRIOT Act (Section 215). Today I am authorizing the declassification and public release of a number of additional documents relating to collection under Section 215. These documents were properly classified, and their declassification is not done lightly. I have determined, however, that the harm to national security from the release of these documents is outweighed by the public interest.

Release of these documents reflects the Executive Branch's continued commitment to making information about this intelligence collection program publicly available when appropriate and consistent with the national security of the United States. Additionally, they demonstrate the extent to which the Intelligence Community kept both Congress and the Foreign Intelligence Surveillance Court apprised of the status of the collection program under Section 215. Some information has been redacted because these documents include discussion of matters that continue to be properly classified for national security reasons and the harm to national security would be great if disclosed. These documents will be made available at the website of the Office of the Director of National Intelligence and at ICOntheRecord.tumblr.com, the public website dedicated to fostering greater public visibility into the intelligence activities of the U.S. Government.

James R. Clapper
Director of National Intelligence

---

1. February 25, 2009 NSA notification memorandum to the House Permanent Select Committee on Intelligence (HPSCI) of compliance incidents identified during an on-going NSA-initiated End-to-End review of its collection of bulk telephony metadata pursuant to Section 215 authorities.

2. March 2009 Internal NSA Memorandum of Understanding required for access and query privileges of data collected through NSA's bulk telephony metadata program under Section 215 authorities.

3. May 7, 2009 NSA notification memorandum to the Senate Select Committee on Intelligence (SSCI) and HPSCI on the status of the on-going NSA-initiated End-to-End review of its collection of bulk telephony metadata pursuant to Section 215 authorities.

4. July 2, 2009 Letter from the Department of Justice (DoJ) to the United States Foreign Intelligence Surveillance Court (FISC), providing notice of the production of NSA's June 25, 2009 Business Records Foreign Intelligence Surveillance Act (FISA) End-to-End Review Report to the Congressional Intelligence and Judiciary Committees.

5. September 10, 2009 NSA notification memorandum to SSCI of presentations made to several FISC judges regarding NSA's bulk telephony metadata program under Section 215 authorities and of the FISC granting the government's request to reauthorize the bulk telephony metadata program and restoring to NSA the authority to query the metadata upon a Reasonable Articulable Suspicion standard without seeking Court approval on a case-by-case basis.

6. October 21, 2009 Joint Statement for the Record by the Director of the National Counterterrorism Center and the Associate Deputy Director for Counterterrorism of the NSA, to HPSCI providing information relating to NSA's bulk telephony metadata program under Section 215 authorities for the USA PATRIOT Act reauthorization.

7. December 17, 2009 Letters from DoJ to Representatives Bobby Scott, John Conyers, and Jerrold Nadler providing notice of Executive branch efforts with the Intelligence Committees to make a detailed report on NSA's bulk telephony metadata program under Section 215 authorities available to all Members of Congress.

8. August 16, 2010 Cover Letter from DoJ for submission of several documents to the Congressional Intelligence and Judiciary Committees relating to NSA collection of bulk telephony metadata under Section 501 of the FISA, as amended by Section 215 of the USA PATRIOT Act.

9. April 1, 2011 Memorandum from NSA to SSCI regarding NSA's receipt of cell site location information test results.

10. September 1, 2011 NSA notification memorandum to the House and Senate Committees on the Judiciary on NSA's collection of telephony metadata under Section 501 of FISA.

- #declassified
- #DNI Clapper
- #NISA
- #Section 501
- #FISA
- #FISC
- #SSCI
- #HPSCI
- #DOJ
- #NCTC
- #Patriot Act
- #metadata
- #Section 215
- #location data

- 3 months ago
- 11
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqyu

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article

October 22, 2013

Recent articles published in the French newspaper Le Monde contain inaccurate and misleading information regarding U.S. foreign intelligence activities. The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false.

While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations. The U.S. collects intelligence to protect the nation, its interests, and its allies from, among other things, threats such as terrorism and the proliferation of weapons of mass destruction.

The United States values our longstanding friendship and alliance with France and we will continue to cooperate on security and intelligence matters going forward.

James R. Clapper
Director of National Intelligence

- #statement
- #DNI Clapper
- #WMD
- #NSA
- #phone records
- #France
- #Le Monde

- 4 months ago
- 20
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqyC

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

Release of Previously Classified October 11, 2013 Foreign Intelligence Surveillance Court Memorandum and Primary Order

October 18, 2013

On October 11, 2013, the Director of National Intelligence declassified and publicly announced that the Foreign Intelligence Surveillance Court had approved the government's application seeking renewal of the authority to collect certain telephony metadata in bulk under the "business records" provision of the Foreign Intelligence Surveillance Act, 50 U.S.C. Section 1861, and that the administration was undertaking a declassification review of this most recent court authorization.

Following a declassification review by the Executive Branch, today the Court released the previously classified Memorandum and Primary Order reauthorizing the collection of bulk telephony metadata under this authority. The Memorandum re-affirms that the bulk telephony metadata collection is both lawful and constitutional.

Shawn S. Turner
ODNI Director of Public Affairs

Via USCourts.gov:

BR 13-158

- Memorandum and Primary Order
- Order (October 15, 2013)
- Order (October 18, 2013)

- #FISC
- #FISA
- #declassified
- #metadata
- #order
- #business records

- 4 months ago
- 8
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqx

TwitterFacebookPinterestGoogle+

Go to LinkPop-upView Separately

Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program

October 11, 2013

As indicated by a declassified court order and amended memorandum opinion published by the Foreign Intelligence Surveillance Court Sept. 17, 2013, the court authorization requiring the production of certain telephony metadata under the "business records" provision of the Foreign Intelligence Surveillance Act, 50 U.S.C. Section 1861, expires Oct. 11, 2013.

Previously on several occasions, the Director of National Intelligence declassified certain information about this telephony metadata collection program in order to provide the public with a more thorough and balanced understanding of the program. Consistent with his prior declassification decision and in light of the significant and continuing public interest in the telephony metadata collection program, DNI Clapper has decided to declassify and disclose publicly that the government filed an application with the Foreign Intelligence Surveillance Court seeking renewal of the authority to collect telephony metadata in bulk, and that the court renewed that authority.

The administration is undertaking a declassification review of this most recent court order.

Shawn Turner
Director of Public Affairs
Office of the Director of National Intelligence

- #statement
- #FISA
- #FISC
- #metadata
- #NSA

- 4 months ago
- 4
- Permalink

Share

Short URL
http://tmblr.co/ZZQjsqxL

TwitterFacebookPinterestGoogle+

? Newer • Older ?

About

Created at the direction of the President of the United States, **IC ON THE RECORD** provides immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence Community.

Follow @IContheRecord

CONTENT CATEGORIES:

- - Official Statements
- - Declassified Documents
- - Testimony
- - Speeches & Interviews
- - Fact Sheets
- - Oversight & Compliance
- - Video

HOT TOPICS:

- - Civil Liberties
- - FISA
- - FISC
- - Section 215
- - Section 702

IN THEIR OWN WORDS:

- - James Clapper, DNI
- - Keith Alexander, Dir. NSA
- - Robert Litt, GC, ODNI
- - John Inglis, Dep. Dir., NSA
- - Alex Joel, CLPO, ODNI

Search this site

This website is maintained by the Office of the Director of National Intelligence.